

What is claimed is:

1. An integrated security information management system, comprising:

5 an Extensible Markup Language (XML) key managing means for performing an interface with an external security information management client based on an XML, authenticating a user, analyzing a request from the integrated security information management client, and requesting a processing to
10 an access control means, an authenticating means or an external public key infrastructure certification server depending on a request kind;

the access control means for providing a user authenticating function, an access authority policy generating function for limited shared data storing means, an access authority confirming function depending on the access authority policy, a shared security information providing function for an access-allowed user, a security information position information providing function, a shared security information registering/deleting/updating function, a shared security information share setting/releasing function, and an
20 XML digital signature / verification / encryption / decryption / communication security function depending on a shared security information processing request from the XML key
25 managing means;

the authenticating means for providing the user authenticating function, a person-in-question authenticating

function, a non-shared security information providing function for the access-allowed user (the person-in-question), a security information position providing function, a non-shared security information registering / modifying / deleting function, and the XML digital signature/ verification / encryption / decryption / communication security function depending on a non-shared security information processing request from the XML key managing means;

the limited shared data storing means for storing and managing security information shared by an object limited depending on a control of the access control means; and

non-shared data storing means for storing and managing security information that should not be shared depending on control of the authenticating means.

15

2. The integrated security information management system as recited in claim 1, wherein in the access authority confirming function depending on an access authority policy of the access control means, if the access control means receives an access request to the limited shared data storing means from the XML key managing means, after a user authentication is performed, the access authority policy corresponding to the requested security information is read to confirm whether or not a user has authority.

25

3. The integrated security information management system as recited in claim 2, wherein when the user registers

the security information through the integrated security information management client, the access authority policy is generated and is continuously and dynamically updated depending on updating/deleting and share setting/releasing of
5 the security information later registered.

4. The integrated security information management system as recited in any one of claims 1 to 3, wherein the access control means and the authenticating means uses a
10 signature received from a security information owner according to the request of the integrated security information management client to further perform a security information share-agency setting function for allowing other users to set/release a share and a function of informing the security
15 information owner of a security information share-agency setting request.

5. The integrated security information management system as recited in claim 4, wherein the access control means
20 and the authenticating means uses a signature and a certificate issued from other users according to the request of the integrated security information management client to further perform a shared security information retrieving function for retrieving the security information shared by a
25 self, a shared security information retrieval confirming function for informing the security information owner of execution of the shared security information retrieving

function depending on the execution, and a shared security information usage log confirming function for confirming a log for a shared security information usage.

5 6. An integrated security information management method, comprising the steps of:

 classifying security information depending on its kind according to a security information registering / updating / deleting request from an integrated security information management client to register/update/delete the classified security information from a limited shared data storage or a non-shared data storage at an integrated security information management system;

15 setting/releasing a share for the security information registered into the limited shared data storage according to a security information share setting/releasing request from the integrated security information management client, and generating/updating a security access authority policy at the integrated security information management system;

20 confirming a request user's authority depending on a security access authority policy according to a shared security information providing request from the integrated security information management client, and then providing corresponding security information for the integrated security information management client at the integrated security information management system;

 authenticating that a request user is a non-shared

security information owner according to a non-shared security information providing request from the integrated security information management client, and then providing corresponding security information for the integrated security information management client at the integrated security information management system; and

generating/verifying a digital signature according to a digital signature generating/verifying request using an XML from the integrated security information management client at the integrated security information management system.

7. The integrated security information management method as recited in claim 6, further comprising the step of:

informing a security information owner of a security information share-agency setting request according to an other owners' security information share-agency setting request from the integrated security information management client to receive acknowledgement, and then allowing other users to use a signature received from the security information owner to set/release the share for corresponding security information at the integrated security information management system.

8. The integrated security information management method as recited in claim 6 or 7, further comprising the step 25 of:

informing the security information owner of a security information verifying request according to an other owners'

security information verifying request from the integrated security information management client to receive acknowledgement, and then providing a verified result of other owners' security information for the integrated security information client at the integrated security information system.

9. The integrated security information management method as recited in claim 8, wherein the security information registering / updating / deleting step comprises the steps of:

a user's requesting an extensible XKMS server of the integrated security information management system for security information registration / update / deletion through the integrated security information management client;

15 authenticating the request user and confirming a security information kind at the extensible XKMS server;

as the confirmation result, if the security information kind is sharable, sending the request to an access control server to register / update / delete the security information 20 from a limited shared data storage; and

as the confirmation result, if the security information kind is non-sharable, sending the request to an authentication server to register / update / delete the security information from a non-shared data storage.

25

10. The integrated security information management method as recited in claim 8, wherein the security information

share setting/releasing step comprises the steps of:

a user's requesting the extensible XKMS server of the integrated security information management system for security information share set/release through the integrated security information management client;

authenticating the request user at the extensible XKMS server, and then sending a security information share setting/releasing request to the access control server, and loading an access authority policy for corresponding security information at the access control server, and then confirming whether or not the access authority policy is set to allow the request user to share; and

as the confirmation result, in case the access authority policy is set to allow the request user to share, reading the corresponding security information from the limited shared data storage to send the read security information to the request user through the integrated security information management client.